INFORMATION WARFARE: Will We Be Prepared When War Comes Home?

CSC 1998

Subject Area - Warfighting

EXECUTIVE SUMMARY

Title: INFORMATION WARFARE: Will We Be Prepared When War Comes Home?

Author: LCDR Gretchen S. Herbert, United States Navy

Thesis: As the United States becomes increasingly dependent on information infrastructures to conduct daily activities, it is also becoming increasingly susceptible to information warfare (IW) attacks. A thorough understanding of the risks and vulnerabilities of an IW attack against the United States is crucial in implementing a credible defense.

Discussion:

The technological advances of the Information Age bring significant advantages in timeliness and efficiency, but incorporating these technologies also brings with it significant challenges to national defense. With its increased reliance on information, the United States must reevaluate its vulnerabilities and methods of ensuring protection of our national interest. The advances in IW capabilities may, in the end, be more beneficial to those countries that could never hope to challenge the U.S. in conventional military strength. It is therefore critical that the U.S. adopts an effective and resilient IW defense.

The importance of information and the advances in associated technologies are going to increase significantly in the future. In order to realize the true benefit of the Information Age, the United States must ensure the availability, reliability and protectability of our information infrastructures. While the nation has been quick to incorporate advanced technologies into its daily routine, the exploration of associated defensive, offensive and legal ramifications of IW has not been as rapid. At present, the U.S. is ill-prepared to defend against a coordinated IW attack on our national information infrastructures.

Recommendation:

To preserve the integrity, availability and security of information systems, an accurate assessment of the nation's current and future vulnerabilities must be formulated and updated. Establishing an information "Red Cell" to conduct wargames that probe national systems and identify inherent weaknesses in their security measures is an immediate step. Additionally, government should allocate sufficient funds into research and development efforts for enhancing computer security and infrastructure protection, and for activating an Information Indications and Warning Center that can accurately assess when an IW attack is attempted, limit its effects, and trace the origin of the attack.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
1998		**00-00-1998 to 00-00-1998**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
INFORMATION WARFARE: Will We Be Prepared When War Comes Home?	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **United States Marine Corps,Command and Staff College, Marine Corps University,2076 South Street, Marine Corps Combat Development Command,Quantico,VA,22134-5068**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**43**	

CONTENTS

I. INFORMATION WARFARE AND DEFENSE OF THE HOMELAND

The United States is becoming increasingly reliant on information and communications systems, not only for the timely and effective execution of military operations, but in the conduct of the majority of public and private sector business transactions and activities. There is little question that the U.S. military is the strongest in today's global arena, but our traditional defenses may offer little protection from information age threats to our national security. Our country's reliance on information and information systems makes it vulnerable in that these systems become lucrative and achievable targets for a weaker adversary who could not challenge the United States militarily. The rapid proliferation and integration of dual-use telecommunications and computer systems have been significant "power equalizers," affording previously rudimentary societies and peripheral powers with access to increasingly sophisticated technology that is on par with U.S. capabilities. A relatively new form of conflict, Information Warfare (IW) capitalizes on the growing advantages and dependencies that information technologies have made possible. Compared to the military forces and weaponry that threatened our national security in the past, Information Warfare weapons are inexpensive and readily available to numerous nations and non-state actors alike.

The technological advances of the Information Age bring significant advantages in timeliness and efficiency, but incorporating these technologies also brings with it significant challenges to national defense. With its increased reliance on information, the United States must reevaluate its vulnerabilities and methods of ensuring protection of our national interests. Geographical separation and superpower status might be of little value for ensuring national security in a world that is globally integrated and interdependent. The advances in IW capabilities may, in the end, be more beneficial to those countries that could never hope to equal U.S. conventional military strength. It is therefore critical that the U.S. adopts an effective and resilient IW defense. Since the end of the Cold War, asymmetrical warfare scenarios have

challenged the U.S. military's operational effectiveness and its ability to successfully attain national objectives. These challenges are magnified when the asymmetrical attacks involve IW tactics and weaponry; the simple act of identifying whether an attack is underway, and by whom, can be insurmountable.

The importance of information and the advances in associated technology are only going to increase in the future. In order to realize the true benefit of information age technologies, the United States must ensure the availability, reliability and protectability of our information infrastructures. This paper will argue that, while the nation has been quick to incorporate information age technologies into its daily routine, the exploration of associated defensive, offensive and legal ramifications of IW has not been as rapid. At present, the U.S. is ill-prepared to defend against a coordinated IW attack on our national information infrastructures. Furthermore, while building a credible defense has been elusive, the problem of orchestrating an effective response has yet to be addressed through significant public discourse.

The U.S. lacks the necessary policy framework to respond quickly, legally and effectively to an IW attack. Although an informational attack may be non-lethal in nature, its disruptive potential to an informationally reliant country can be immense and potentially catastrophic. Despite this significant vulnerability, the U.S. political and military arsenal at present lacks direction on appropriate retaliatory responses that will be commensurate with the damage inflicted by an IW attack, and that will withstand public and international evaluation and scrutiny.

II. WHAT IS INFORMATION WARFARE?

Perhaps the difficulties in grasping the national security implications of information operations and information warfare stem from the lack of consensus on their very definition and what they encompass. The Department of Defense's definition is both conveniently broad and frustratingly inadequate. It defines IW as, "actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while leveraging and defending one's own information, information-based processes, information systems, and computer-based networks."[1] Correctly, information is not only the target of attack, but can also serve as the weapon, the resource and the medium as well. The military frequently equates IW to little more than an updated version of Command and Control Warfare (C2W) which focuses on purely military applications of Electronic Warfare (EW), Operational Security (OPSEC), Psychological Operations (PSYOPS), Operational Deception and Physical Destruction. More than a C2W synonym, IW has grown to encompass the political, economic and sociological aspects of national power and has become an inviting avenue for threatening our critical national interests at home. The scope and breadth of IW necessitates that information and information links be categorized as strategic national assets that must be protected.

Noted futurists Alvin and Heidi Toffler link the growing importance of (and society's growing dependence on) information and knowledge to fundamental changes in societal priorities and actions, both in making wealth and in making war.[2] They have divided civilizations into three distinct "waves" separated by technological advances and informational sophistication. First Wave societies are products of the Agrarian Age and as such, are

---

[1] Joint Chiefs of Staff, Joint Pub 1-02, Department of Defense Dictionary of Military and Associated Terms (Washington, DC: GPO, January 1998), 212.

[2] Alvin and Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century (Boston, MA: Little Brown and Co, 1993), 18-78.

inescapably tied to the land. Their method of warfare was limited, prolonged and seasonal. The Industrial Revolution marked the evolution of many societies into the "Second Wave" of advanced civilizations. As industrial mass production transformed nations, it also transformed their way of preparing for and waging war. Limited warfare objectives were replaced by those of unlimited aims and increasing an army's mass, range and lethality predominantly determined success on the battlefield. The United States is on the verge of fully entering the final wave of the Tofflers' three wave model, that of the post-industrialized, Information Age civilization, where the intangible assets of information and knowledge are both vital resources, marketable commodities, and the very vehicles for making wealth and making wars. In their view, information technology and the knowledge it affords will increasingly dominate, and eventually supplant, the importance of raw materials and industrial-age products. The politics of the future will focus on Information Age concerns oriented towards the storage, protection and exchange of information, vice the protection and marketing of more tangible assets. Likewise, in warfare, our ability to employ and exploit battlespace information, and manipulate, disrupt or destroy an adversary's access to information, will be infinitely more important than the mass and lethality of Second Wave forces and weaponry.

The Gulf War has been touted as the first Information War.[3] Certainly, when compared to past wars, the forces allied against Iraq came the closest to harnessing and applying many of the battlespace advantages of information technologies and precision weaponry. Operation DESERT STORM clearly demonstrated the lethal effectiveness of integrated weapon systems and information superiority in combat. However, according to the Tofflers' Wave model, the Gulf War represented a hybrid, or perhaps, a transition.[4] The Gulf War, they argue, was an example of Second Wave warfare (Iraq) waged against a pseudo-Third Wave force (Allied coalition) which used the weapons of the industrialized age, enhanced with the knowledge and precision afforded by the information age. Information warfare capabilities were successfully

[3] Campen, Alan D, The First Information War (Fairfax, VA: AFCEA International Press, 1992), 3-4.
[4] Tofflers, 3.

demonstrated as potent enhancements to conventional warfare weaponry, albeit against an adversary who either neglected to, or was incapable of, employing any IW offense or defense of his own. The next drill might not be as easy. More likely, potential adversaries will have taken note of the U.S. military's technological superiority and in the future, seek to avoid it completely, choosing instead an asymmetrical approach that will circumvent our proven capabilities and probe at our potential weaknesses.

The myriad of military and civilian implications of information warfare are delineated by what John Arquilla and David Ronfeldt have coined "cyberwar" and "netwar."[5] They describe cyberwar as conducting military operations according to information-related principles, much along the lines of our C2W concept. The result of a successful cyberwar campaign would turn the balance of information and knowledge, and ultimately the war, in one's favor, even if the balance of forces were predominantly with the adversary. On a broader scope, netwar is information-related conflict at the grand strategic level, waged by every element of national power, with such tactics as manipulation of the media, infiltration or infestation of computer networks and databases, political and cultural subversion, economic upheaval, and psychological campaigns focused on the private sector.

Other scholars have expressed similar views on the expanding nature of IW. Winn Schwartau defines IW as an "electronic conflict in which information is a strategic asset worthy of conquest or destruction."[6] He further delineates three classes of IW as attacks on personal information systems (Class 1), attacks on corporations and businesses (Class 2) and the national strategic level of global information attacks (Class 3). The potential targets of IW attacks are more complete and ominous. "Information warfare," Schwartau continues, "is waged against industries, political spheres of influence, global economic forces, or even against entire countries. It is the use of technology against technology...about turning information against its

---

[5] John Arquilla and David Ronfeldt, "CyberWar is Coming," Comparative Strategy, vol. 12, no. 2 (Spring 1993): 150.

[6] Winn Schwartau, Information Warfare: Chaos on the Electronic Superhighway, (New York: Thunder's Mouth Press, 1994), 13.

owners...about denying an enemy the ability to use both his technology and his information."[7] This incorporation of internal national security threats is important in broadening the perspective of, and attention to, IW implications beyond the military applications. Unlike a typical warfare scenario, the traditional "theater" is expanding and no longer incorporates solely the close, deep and rear areas of operations. It includes the homeland as it never has before. While airstrikes during WWII targeted the German and British homelands, they were the result of a broadening offensive campaign within an ongoing war effort. With IW, there is no "front line," and there may be no preliminary indications and warning to an attack. Many have drawn another WWII parallel, equating an IW attack to a "electronic Pearl Harbor," where the homeland is once again vulnerable.[8]

The impact of IW on modern warfare is the subject of ongoing debate. The spectrum of potential IW applications range from playing only a supporting role -- enhancing current doctrine, tactics and employment of weapons -- to the vision of clean, bloodless warfare in which the enemy can be defeated without a shot being fired. Some vehemently protest that technological advancements and information dominance will never replace the basic necessity of troops on the ground. General Van Riper and General Scales expressed concern over "recent claims that technological supremacy will allow the United States in the future to abjure the use of ground combat forces in favor of delivering advanced precision weaponry from platforms remote from conflict areas."[9] Others see the humanitarian possibilities of a casualty-free war of information as infinitely more palatable than the conventional alternative. "At the heart of the concept of IW is the concept of achieving military objectives with the absolute minimum of

---

[7] Ibid, 291.

[8] Martin C. Libicki, "Protecting the United States in Cyberspace," in Cyberwar: Security, Strategy, and Conflict in the Information Age, eds. Alan D. Campen, Douglas H. Dearth, and R. Thomas Gooden (Fairfax, VA: AFCEA International Press, 1996), 98.

[9] Lt Gen Paul K. Van Riper and Maj Gen Robert H Scales, Jr, "Preparing for War in the 21st Century," Parameters vol. 27, no. 3 (Autumn 1997): 4.

force application...imposing [our] will without the cost of occupying the enemy's territory. Clausewitz's fixation with physical destruction and annihilation may be outdated."[10]

More than likely, IW's role in the future of warfare will incorporate elements of both arguments, neither slave to current warfighting tactics and weaponry, nor the panacea weapon of the future - capable of destroying the will of the enemy without the need of the "physical punch" afforded by conventional forces. The structure, tactics and doctrine of future forces may be drastically different in size and organization due to their information edge, but their presence will still be required. The optimal role and placement of IW in the "escalation to conflict" spectrum is still unknown, but the applicability of IW as an ongoing activity in peace, crisis and war is entirely feasible. Its most effective application may be as a precursor to the escalation to arms, as battlefield preparation or as a non-lethal offensive capability to be employed after diplomacy and negotiations fail and before mobilization of forces begins. In this era of reduced spending and budgetary restrictions, IW as a forerunner to armed hostilities, if effective, would be attractive.

The basic concept of IW is not really new to warfighting. Rumor, propaganda, deception and misinformation were all identified by Sun Tzu as appropriate and necessary adjuncts to the battle. The volume, availability and accuracy of information in today's battlespace, however, has raised the importance of deception operations and information denial to an unparalleled position in the warfighter's arsenal. Correspondingly, the *nature* of deception operations has changed from creating a false "physical reality" for the enemy to discover, such as with the diversionary feint of Amphibious forces during the Desert Storm campaign, to creating a false "virtual reality", manufactured by manipulating or deceiving the enemy's database to achieve the same effects.[11] Another emerging feature of IW is the ascendancy of knowledge over lethality -- the value of information in war might soon outpace the value of a powerful weapons system.

---

[10] Douglas Dearth and Charles Williamson, "Information Age/Information War," in Cyberwar, 27.

[11] Michael L. Brown, "The Revolution in Military Affairs: The Information Dimension," in Cyberwar, 46.

John Arquilla and David Ronfeldt see the information impact in 21st century warfare as the equivalent of the 20th century Blitzkrieg.[12] The traditional importance of obtaining information and eliminating uncertainty in warfare might become the prevailing essential element for future confrontations. The object would not be to kill the opposing force, but to paralyze its entire national infrastructure. Information warfare in the 21st century will focus less on a destructive, attrition-based war and more on the destructive *effects* of information deprivation.

The merits of IW should not be examined without also exploring its potential shortcomings. If IW does prove to be the compelling force of future wars, it is critical to identify not only those powers poised to exploit the offensive opportunities of an IW environment, but also those societies that would be most vulnerable to the crippling elements of an information attack. The potential impact of IW will be directly proportional to the sophistication of the targeted nation and its corresponding reliance on information systems. An informationally advanced Third Wave society that has learned to leverage the capabilities of information in crisis and peacetime will be the most vulnerable to attack and exploitation. Even if associated system disruptions are only temporary, their effects will be far more troubling and problematic for the technologically advanced. To properly identify the defensive measures required to preempt or minimize the impact of such an attack, an analysis of the inherent risks and vulnerabilities of an informationally-dependent Third Wave society, such as the United States, is a required first step.

[12] Arquilla and Ronfeldt, "Cyberwar is Coming," 160.

III. RISKS AND VULNERABILITIES

> The national security posture of the United States is increasingly dependent on our information infrastructures. These infrastructures are highly interdependent and are increasingly vulnerable to tampering and exploitation. Concepts and technologies are being developed and employed to protect and defend against these vulnerabilities. We must fully implement them to ensure the future security of not only our national information infrastructure, but our nation as well.
>
> President Bill Clinton[13]

Government leadership has recognized both the significant enhancements and the disruptive potentials of a globally-networked society. Advancements in information technologies have been welcomed and incorporated into commercial and governmental sectors alike. However, as is often the case with state-of-the-art technologies, their vast potential for improved efficiency and speed is embraced before any detrimental aspects are explored. Today, the United States finds itself fully immersed in the Information Age; day-to-day activities and operations are fully dependent on the quality and accessibility of our information systems and networks. But while facilitating many functions, the information edge brings with it significant national security challenges. As Martin Libicki observed, "Information systems are interconnecting via phone and E-mail. Interconnection saves manhours, promotes workplace collaboration, and permits remote management, but also permits havoc to seep in from outside, or even abroad."[14] Our nation's transition into a knowledge based society, while enabling our military to achieve apparent information dominance on the battlefield, has left the homeland vulnerable to attack and created dilemmas and unanswered questions about our defensive readiness.

The National Information Infrastructure (NII) is the informational backbone to a myriad of vital national networks. The successful operations of our financial institutions,

---

[13] The White House, A National Security Strategy for a New Century (Washington, DC: GPO, May 1997), 14.

[14] Libicki, Cyberwar, 92.

communications and public switched networks (PSN), power grids, transportation systems, air traffic control, government and defense networks, private corporate and institutional networks, are all dependent upon a robust and fully functional NII. A successfully coordinated IW attack could target and disrupt the information and networks that support crucial daily operations of commercial, governmental and military systems. In an information-based economy, denying access to information transfers can quickly create economic instability. Crippling the NII in turn would instantaneously cripple military information networks as well. The Defense Information Infrastructure (DII) which "rides" on the NII, connects all Department of Defense (DoD) mission support, command and control, and intelligence computers and systems. With 95 percent of DoD communications dependent on the health of the NII, networks over which DoD exercises little control, the need for ensuring the health and robustness of the NII is fundamental. The NII itself is increasingly connected with and dependent upon the transnational collection of networks, the Global Information Infrastructure (GII), further linking national defense to international entities.

Just how vulnerable are our systems to attack? A study by the Center for Information Systems Security tested U.S. systems' vulnerability to intrusion using computer "hacking" tools which were freely available on the Internet. The study reported an 88 percent success rate in penetrating unclassified government systems. Only 4 percent of successful penetrations were detected by the organizations under attack. Of those organizations, only 5 percent reacted to try and identify or terminate the attack.[15] In 1995, more than 250 unclassified DoD systems were known to have been penetrated by outsiders. Essential information supported by those systems included weapons and supercomputer research, logistics, finance, procurement, personnel management, payroll and military health systems.[16] In a 1996 study, the General Accounting Office (GAO) reported to Congress that as many as 250,000 hacker attacks were being launched

[15] Robert Ayers, "Defensive Information Warfare: A Maginot Line in Hyperspace," OSS Notices vol. 2, no. 10 (30 Dec 94): 10.

[16] Kenneth A. Minihan, "Intelligence and Information Systems Security: Partners in Defensive Information Warfare," Defense Intelligence Journal vol. 5, no. 1 (Spring 1996): 15.

annually against DoD computer systems.[17] The GAO further estimates that more than 120 countries already have or are developing computer attack capabilities. Computers are now weapons systems, capable of "launching" such virtual missiles as viruses, logic bombs, worms, Trojan horses, and demons.[18] Despite highly publicized computer attacks, DoD still operates primarily in the reactive mode without a uniform policy for assessing risks, protecting systems, responding to attacks or assessing battle damage.[19]

Information warfare attacks against the United States, most probably initiated by non-state actors, are increasingly feasible due to the low-cost, high pay-off and virtual guaranteed anonymity to the attacker. National and subnational groups that do not command large military establishments can still wage effective IW.[20] An IW offensive capability would be both attractive and feasible to many because of its inexpensive "arsenal" (often little more than a computer terminal and modem interfaced into the GII), especially when compared to the cost of developing, procuring and sustaining an advanced conventional military capability. Information technologies and their ready availability are significant "force equalizers" that could quickly recalibrate the balance of power in the information realm. *Time* magazine speculates that hackers may be the new mercenaries of the future.[21] During the Gulf War, a group of Dutch hackers offered their services to Iraq, promising to disrupt the U.S. military's deployment to the Middle East for one million dollars. Saddam Hussein declined. While these offered disruptions may not have changed the outcome of the war, they most certainly would have protracted it,

---

[17] Kenneth Allard, "Assessing Byte City," Washington Quarterly (Spring 1996): 88.

[18] A Virus is a program which attaches itself to resident files, spreads to other files it comes into contact with, and potentially erases or disrupts the files. Logic bombs are programs that lie dormant until a predetermined time or condition, when they are activated, and alter, deny, or destroy data. Worms are nuisance files which grow within an information system, altering files, taking up memory space and/or overwriting other files. Trojan Horses are codes hidden within a computer system and can authorize access to the system or alter, deny or destroy data. Demons are programs which record all commands entered into a system and, when queried, can reveal access codes, encryption keys, etc.

[19] Charlotte Adams, "DoD Information Takes Big Strides but Still Lags Behind Threats," Military & Aerospace Electronics vol. 8, no. 1. (January 1997): 17.

[20] Walter B. Wriston, "Bits, Bytes and Diplomacy," Peaceworks: Keynote Addresses From the Virtual Diplomacy Conference, September 1997, 7.

[21] Douglas Waller, "Onward Cyber Soldiers," Time, 21 August 1995, 44.

increasing the possibility of escalating U.S. casualties, losing public support at home, and jeopardizing a fragile alliance.

National centers of gravity will increasingly be found in the civilian sector. Adversaries looking for a high value target with negligible to nonexistent retaliatory risk, need only conduct a synchronized electronic attack against several vital, yet unprotected information nodes.

> Our most vexing future adversary may be one who can use technology to make rapid improvements in its military capabilities that provide asymmetrical counters to US military strengths, including information technologies.... We anticipate the probability of facing technological or operational surprise will increase in the period ahead.[22]

IW attacks can take the form of "hard kill" tactics (sending a cruise missile into an enemy's vital C2 nodes), "soft kill" (jamming frequencies or infecting systems with viruses that wipe out all information within the systems), psychological attacks (media reports and broadcasts that break the morale and will of enemy forces or the public), and a spectrum of alternatives in between (surreptitiously manipulating or changing data, sending false signals, stealing mission critical information, etc.). The majority of these methods can span the conflict spectrum from peace to war and take the form of either overt or covert attacks.

That which makes us strong can also make us weak. As the most networked, most sophisticated, and most advanced information age society, the United States is also the most vulnerable to an all-out coordinated information attack. Our heavy reliance on our information infrastructures make them lucrative and under-defended targets. Rapid technological advances and the eager assimilation of them into daily tasks and functions, have outpaced the ability of both the government and the private sector to incorporate the necessary security measures and defensive safeguards into procedures and doctrine.

In 1995, the Rand Corporation was asked to provide and exercise an analytic framework for identifying key IW issues, exploring their consequences and providing starting points for

---

[22] Chairman, Joint Chiefs of Staff, Joint Vision 2010 (Washington, DC: GPO, May 1996), 10-11

future IW policy development. Rand staged a series of information wargames to assess the vulnerabilities and variations of an information attack against the United States and its allies.[23] Entitled "The Day After...In Cyberspace," the scenario depicted an attempt by Iran to drive up oil prices and forcibly coerce Saudi Arabia into cooperation. As the scenario developed, intelligence reports indicated that Iran had a growing information warfare capability -- an assessment that was promptly validated by unexplained computer crashes, phone service disruptions, illegal funds transfers, and a breakdown of automated transportation controls. Bringing the chaos closer to home for its military participants, the scenario also detailed a hamstrung military unable to mobilize because the computerized Time Phased Force Deployment Data (TPFDD) file was attacked by a computer worm that corrupted all the coordinating data on the movement of troops, weapons, equipment, and other essential supplies.

Among its findings, the wargame highlighted seven characteristic features of what Rand termed "strategic information warfare."[24] Those factors included:

- Low entry costs -- Unlike traditional weapons technologies, information-based attack techniques did not require large financial resources or state sponsorship for building a credible "arsenal". Sometimes nothing more than a computer, a modem, and access into a worldwide network was needed.

- Blurred traditional boundaries -- In cyberspace, the distinction between private and public domain, and national and international borders were often indistinguishable. Likewise, the ability to differentiate between warlike, criminal, and merely "mischievous" behavior was problematic and often inconclusive.

- Expanding role of perception management -- Data manipulation complicates accurate assessment of what is genuine and what is "doctored."

- Intelligence collection challenges -- Identifying intentions, likely target sets, or even potential adversaries is difficult in IW defense. There is no enemy order of battle (OOB) to use as a guide in determining intentions or in refining estimates of enemy strengths and capabilities.

---

[23] Roger Molander, Andrew Riddile and Peter Wilson, Strategic Information Warfare: A New Face of War (Santa Monica, CA: The Rand Corp., 1996), 1-10.

[24] Ibid, 16.

- Tactical warning deficiencies -- The majority of systems and networks are not adequately protected or equipped to notice sporadic or small scale intrusions which can mask the fact that a system is even under attack.

- Difficulties in building or sustaining coalitions -- Reliance on coalitions with inferior information security safeguards is likely to increase vulnerabilities to the U.S. security posture.

- Vulnerability of U.S. homeland -- The most ominous conclusion of the Rand study revealed that information technologies have rendered even spatial distances irrelevant and have eliminated the previous notion of "protected sanctuary."

Former CIA director John Deutch also acknowledged that the United States was not well organized as a government to address the cyberspace threat.[25] He identified the likelihood of an IW attack as one of the top threats to U.S. national security, ranking it third behind those of weapons of mass destruction (WMD) and the proliferation and terrorist use of nuclear, biological and chemical (NBC) weapons. The ability of an adversary to launch untraceable attacks from anywhere in the world, or from within the United States, was significant. Likewise, U.S. government information security policy was identified as lagging far behind the capabilities of modern information transfer and storage systems.[26]

Another significant vulnerability of a globally networked information infrastructure is the potential ease with which public perception or media reporting can be manipulated. Our society's hunger for rapid, late-breaking news reports, sometimes termed the CNN-effect, has already put substantial pressure on both government leadership and media management alike. The information revolution is taking the initiative in policy making away from the government. The media is able to report international events and global developments directly to the public, often before national decision-makers have time to assess, much less respond to those developments. Indeed, the media often provides the primary source of a decisionmaker's information. The symptom has necessitated that the political decision cycle be shortened considerably, compelling government to react to increasingly complex matters in significantly

[25] John Mann, "Cyber Threat Expands with Unchecked Speed," Aviation Week and Space Technology, 8 July 1996, 63.

[26] Ibid, 64.

less time. "How policy makers react to and cope with the fact that their hands are being forced by the mass media has created a new set of challenges for governance and diplomacy."[27]

The national appetite for the late-breaking news story has complicated the job of the news man as well and created yet another seam for belligerent exploitation. The sheer quantity of available information has become overwhelming, a condition which many military intelligence analysts on the battlefield will attest to. The increased demand for news and information greatly exceeds the capacity of news organizations to independently obtain, scan and evaluate news worldwide.[28] The inundation of information could feasibly lead to quality assurance breakdowns in verification of a story's accuracy and validity. The potential danger here would be the publication of a false news item, supplied by a foreign government or non-state organization with the aim of discrediting governmental leadership, advertising "crimes against humanity" allegedly perpetrated by military forces overseas, or creating public concern or fear over the destabilization of a variety of international interests.

Modern technologies and global networks have magnified the ability of an organization, state or individual to transmit a message to large-scale, dispersed audiences. The ability of a single actor to exert substantial leverage via IW significantly changes the relative balance of power between the individual and the state. The Internet, for example, facilitates the free flow of information and exchange of ideas. The fact that information placed on the Internet is non-regulated and non-discriminatory should make most readers question the credibility and accuracy of all "news" found there, but that may not always be the case. Perception management would effectively equate to PSYOPS at home. An adversary's IW campaign might side-step the military and directly target the U.S. public. Our experiences in Somalia showed just how critical public opinion and support is in the accomplishment of our military objectives.

---

[27] Richard H. Solomon, "The Information Revolution and International Conflict Management," Peaceworks: Keynote Addresses from the Virtual Diplomacy Conference, September 1997, 4.

[28] John W. Rendon, Jr, "The Information Warrior," in The Information Revolution and National Security, ed. Stuart J.D. Schwartzstein (Washington, DC: Center for Strategic and International Studies, 1996), 58.

The technology of nuclear weapons primarily was the governments domain. The domain of IW, however, is increasingly the domain of commercial industry - the government does not have near-exclusive control. An information age vulnerability of the military establishment is their extensive acquisition of dual-use, commercial-off-the-shelf (COTS) electronics, equipment, software and networking protocols. During the Cold War, military systems and "weapons of choice" were created with components that had no civilian counterparts of similar technology.[29] A restrictive defense budget, combined with the availability and relevance of current commercial information technologies, has moved DoD into the position of being "just another customer" of an information technology business driven by commercial priorities and policies. When components to precision guided missiles and satellite technology can be readily purchased in the commercial sector, it may not be long before potential adversaries or even rival companies are able to design counter technologies that could potentially deactivate or disrupt the accurate functioning of our military systems.

Information age threats are likely to be more dispersed, nonlinear and multi-dimensional than our threats of the past. Power is migrating to small, non-state actors who can organize and coordinate via information networks. Their decentralized organization and ability to remain anonymous will make them particularly immune to tracing or retaliatory action by the U.S. Many question whether the shock value or the responsiveness of an information attack are adequate in meeting the requirements of the media-courting terrorist. Terrorist activity has become increasingly violent and indiscriminate over the years and the prospect of resorting to a relatively non-lethal, albeit widely disruptive, attack may be unattractive to terrorists.

Brian Jenkins speculated that the chance of terrorists adopting purely information warfare tactics was unlikely. He viewed that IW attacks "do not produce immediate, visible effects. There is no drama. No lives hang in the balance. There is no bang, no blood. They satisfy

---

[29] Jeffrey R. Cooper, "Another View of Information Warfare: Conflict in the Information Age," in The Information Revolution and National Security, 109.

neither the hostility nor the publicity hunger of terrorists."[30] Others feel that resorting to IW tactics would be "beneath" the political and deadly aspirations of a terrorist movement. Some view it almost as if a purely non-lethal attack would bring discredit to the terrorist and raise questions as to his bravery and commitment to the "cause." As researchers for the Center for International Security and Arms Control (CISAC) eloquently stated, "Until the impact of an electronic attack upon the target audience breaks the stigma of being perpetrated by delinquent adolescents, terrorists will probably shun such attacks."[31]

Indeed, at present, it does appear that most electronic break-ins are performed by under-age, computer wizards, with no more motivation than the thrill of hacking into secure systems without being caught. The *Washington Post* recently reported on an electronic assault to at least eleven U.S. military computer systems, in what Deputy Defense Secretary John Hamre called "the most organized and systematic attack" on U.S. defense networks discovered thus far.[32] The sequence of attacks spanned over a week, and passed through a variety of other systems, both domestic and international, before reaching the DoD targets. It was reported that one of the computer nodes used in the attack was a computer system in the United Arab Emirates, although investigators had ruled out the UAE government as a suspect.[33]

As investigations progressed, it was reported that law enforcement agents had traced the source of the systematic attacks back to a group of hackers which included two high school sophomores from Northern California. The group had also entered computer systems at several universities and federal research facilities, including Brookhaven National Laboratories, the University of California at Berkeley, and the Massachusetts Institute of Technology's fusion labs, some of which performed nuclear weapons research.[34] While reports thus far do not indicate

---

[30] As reported by Kevin Soo Hoo, Seymour Goodman, and Lawrence Greenberg, "Information Technology and the Terrorist Threat," Survival vol. 39, no. 3 (Autumn 1997): 145-6.

[31] Ibid, 146.

[32] Bradley Graham, "11 U.S. Military Computer Systems Breached by Hackers This Month," Washington Post, 28 February 1998, Sec. A1.

[33] Ibid, Sec. A1.

[34] Rajiv Chandrasekaran and Elizabeth Corcoran, "Two California Teens Suspected of Breaking Into Government Computers," Washington Post, 28 February 1998, Sec. A6.

that any classified material was compromised, they do call attention to the vulnerability of even those governmental systems that are regulated by certain measures of computer security -- seemingly to no avail. Not surprisingly, the break-ins "aroused concern among officials worried about the possibility of electronic sabotage as a means of terrorism or warfare."[35]

It should not come as much of a revelation to anyone that the ease with which a thrill-seeking teenager breaks into a governmental system could be easily duplicated by a more politically or financially motivated attacker. Orchestrating an IW attack would be infinitely easier, harder to trace and less risky to the terrorist than building a conventional bomb or NBC weapon. For those weapons, the attacker must be present to plant, launch, or detonate the weapon. An IW attack can be conducted from the sanctuary and relative security of one's home and present little if any risk to the attacker. While it appears unlikely that any terrorist strategy will migrate to one of purely information warfare attacks, it is increasingly probable that some manner of cyber terrorism will be adopted by these groups, to supplement more conventional terrorist methods. By conducting isolated or coordinated cyber attacks on national infrastructures, terrorist organizations can systematically and visibly damage the strength, credibility, and cohesion of a government -- not only physically, but in the eyes of the watching public. The most damaging aspect of terrorists adopting information warfare tactics could be the perceived image of a great nation reduced in stature, vulnerable, defenseless and confused in the wake of an information attack. The possibility of receiving so rich a reward may be too tantalizing for the terrorist to pass up.

The increasing vulnerabilities of an information-based society is disturbing, but do the potential threats outweigh the obvious advantages of incorporating information technologies into public and private sectors' ways of conducting business? It would be a mistake to let the predicted, although as yet, largely undemonstrated, destructive nature of information attacks to override the benefits and positive enhancements these info-age technologies can afford. A better

---

[35] Ibid, Sec. A6.

strategy is to move towards a comprehensive defensive posture that will minimize the affects of an information attack, without curtailing future growth and development in information age technologies. Identifying potential critical requirements, vulnerabilities and risks is the necessary first step in developing a defensive information strategy that both safeguards U.S. information and critical information-related systems, and preserves our "freedom of movement" within the national information infrastructure.

IV. DEFENDING AMERICA

An ironically frustrating feature of the post-Cold War era is that the loss of the single, megalithic threat of the Soviet Union has spawned instability and, as a result, hosts of less menacing but no less urgent threats to U.S. national security and global stability. Many of these "lesser" threat nations and factions have either already acquired an IW capability, or are well on their way to procuring one. Unlike NBC weapons technology which, although proliferating, is spreading at a slow and somewhat monitorable pace, the proliferation of information technology is rapid and unchecked. The dual-use nature of the majority of information technology would make tracking, monitoring and restriction of its sale both impractical and undesired. With the number of potential adversaries and IW methods increasing daily, what does the United States need to protect itself from a devastating IW attack?

Just as the threat of nuclear war forced the U.S. to develop a new national policy focused on defending America from that new threat, the emergence of an IW threat demands a similar restructuring of our defensive posture. This time, however, the burden of the defensive strategy cannot rest solely on the backs of the government and military. The commercial sector needs to be actively involved in both the planning and the implementation of an effective IW defense, just as the information infrastructures themselves, both public and private, are inextricably intertwined. Ours is a mutual interdependence of vulnerabilities that calls for a mutual interdependence of solutions.

The very nature of security has changed in the information age. Protecting the confidentiality of information while it is transmitted and while it is stored has always been important, but with networked infrastructures, the problem is significantly complicated; systems themselves are now vulnerable to attack and intrusion. Software viruses, denial of service, alteration or destruction of data, all increase the scope of IW defensive responsibility. Harkening back to basic counter-intelligence or false intelligence dilemmas, networked systems can also

mask the actual originators of information and compound problems in ensuring whether all nodes that received transmitted information were, in fact, intended recipients.[36]

The most challenging aspect of defending against an IW attack might well be in actually identifying the responsible agent for developing a comprehensive defensive IW policy. The rapid growth of "cyberspace" has blurred the lines of local, national and international authority over the activities conducted there.[37] Likewise, the global nature of many information networks will cause difficulty in reaching a consensus in the international community on just what level of security will be required to ensure an effective or desired defense. International agreements designed to prevent the waging of IW might be difficult to establish as traditional U.S. allies openly admit to waging *some* subset of IW, i.e., targeting industries for espionage or competitive advantages in the private sector.[38] Gaining international support for a unified ban on IW attacks might well require drawing the difficult distinction between IW waged for political intentions vice IW waged for economic intentions. While either type of attack could ultimately prove equally damaging to U.S. national security, international aversion to economically-motivated attacks might not exist; establishing a global consensus and international censure of such attacks might prove insurmountably problematic.

Even domestically, there is likely to be widely differing opinion on the appropriate degree of protection required for our national informational security. The very strength of our information infrastructures is the unrestricted, far-reaching and unencumbered exchange of information between all nodes of the network. Likewise, the exchange of technological data enables networks and applications to grow and improve. These same positive enhancements

---

[36] Kenneth A. Minihan, "Intelligence and Information Systems Security: Partners in Defensive Information Warfare," Defense Intelligence Journal vol. 5, no. 1 (Spring 1996): 17.

[37] Richard O. Hundley and Robert H. Anderson, Security in Cyberspace: An Emerging Challenge for Society, P-7893 (Santa Monica, CA: The Rand Corp., Dec. 1994), 5.

[38] Matthew G. Devost, National Security in the Information Age, MA Political Science Thesis (Burlington, VT: University of Vermont, May 1995) 19.

exponentially increase the entry-points of and resources for potential attacks. What has resulted is a clash between two often contrary American priorities: national security and civil liberty.[39]

A truly effective IW defense would require massive governmental intrusion into private systems. The civil-libertarian implications of such an approach would be massive. Are we prepared to surrender personal freedoms in exchange for an impenetrable IW defense? Efforts to regulate the exchange of technological data or restrict the interdependence of information infrastructures would raise First Amendment issues, potentially negate the benefits of society's Third Wave advancements and, on the most commercial level, result in higher prices, decreased efficiency and reduced availability of national services. The step backwards in the interest of national security, especially in the absence of a looming, proven threat, might be too much for the public to accept. As Matthew Devost argues, "Though there may be security through autonomy, the benefits of that security do not exceed the costs of disconnecting from the global network."[40]

The *modus operandi* also differs greatly between industry and government, further magnifying the difficulties in agreeing on a unified NII defense. While national security planners prefer to circumvent rather than manage risk during critical operations, most private sector CEOs would view DoD network standards of protection far in excess of their requirements. Furthermore, the massive fiscal investment to bring all of industry's infrastructures up to DoD's network protection standards would have no visible short or long term financial return on the private sector's investment -- signaling the death knell of any such proposition.

Effective computer security programs are becoming more critical in safeguarding the systems that provide essential governmental services. Data encryption, virus checkers, multi-level security and establishing firewalls that restrict unauthorized access into classified systems

---

[39] Alfred A. Jones, "Information Security: Planning for the Deluge," in The Information Revolution and National Security, 37.

[40] Devost, 25.

have long been common in the DoD environment.[41] But while these methods afford protection for the information contained within and transferred between databases, they don't protect the systems themselves from potential disruption resulting from their interface with other non-secure networks. Regardless of what level of information security might be religiously practiced within DoD, overall infrastructure security will only be as strong as its weakest link. If the center of gravity and critical vulnerabilities of a nation's strength shift from elements that the military can control to those outside the Defense Department's traditional sphere of influence, then the national defensive posture must be retooled.

A new defensive strategy requires a symbiotic relationship between the military and the private sector. With the correct approach, both sides can benefit. By articulating its security requirements and providing governmental incentives and tax breaks, policy makers can minimize IW vulnerabilities while industry can expect financial assistance for research and development that will not only benefit its governmental customers, but the majority of private sector customers as well. Actively tapping into commercial ingenuity and flexibility in addressing critical information security issues is crucial for a number of reasons. First, governments are no longer fully sovereign in the world of information. To date, confusion over appropriate jurisdiction and the level of protection required has greatly limited assignment of defensive responsibilities. As yet, there is little consensus as to which governmental agency should be taking the lead in developing a credible IW defense. Departments of Defense, Justice, Energy, Commerce, Treasury, etc, all have a substantial stake in both accurately identifying our nation's risks and minimizing its susceptibility to an IW attack.

Without any visible proprietary sentiments and preconceived allegiances to hamper our efforts, national efforts can best be served by encouraging a national "brain storming" forum for identifying appropriate and feasible solutions to our defense requirements. A second, more compelling reason for including the private sector in devising our national info-defense is the

---

[41] Firewalls are "filters" that guard interfaces between networks, allowing limited interaction between systems on a strictly controlled basis to ensure protection of sensitive material.

very reason DoD turned to COTS technology in the first place: budgetary restrictions and a hopelessly protracted acquisition cycle are not conducive to procuring state-of-the-art technological defensive tools immediately, when they might most be needed. Put more concisely by IW expert Alan Campen: "Coupling the 18 month half life of information technology with our 15 year defense acquisition process yields the horrific prospect that our forces could easily be technologically 'leap-frogged'."[42]

Both active and passive defensive measures can be pursued to form a credible policy. Passive protection involves hardening computers and networks to increase their resistance to attack, enhancing firewalls, implementing encryption, safeguarding passwords, and increasing computer-security awareness. An even more important requirement is developing techniques that monitor cyberspace activity, while protecting personal civil liberties, to detect intrusions, thwart attempts to tamper with data, and trace attempted break-ins back to their points of origin. These active measures utilize employment of agents in analyzing methods of intrusion and tracking the source.[43] Agents are mobile, intelligent software codes that "roam" a network looking for unusual activity, isolate intrusions, conduct limited repair to software damage, and "report back" to system managers on any suspect findings.

The role of the government in providing guidance and direction in establishing an effective national defense is not new to the protection of information transfer. The National Communications System (NCS) was established in 1963 after the Cuban Missile Crisis revealed that the nation's telecommunications infrastructure was an essential component in both deterrence and recovery in the face of a major attack.[44] That same realization in regards to our reliance on computer networks is reflected in new attention to "upgrading" our national laws. Legal systems are struggling to keep pace with technological advances and the emergence of

---

[42] Alan D. Campen, "Rush to Info-Based Warfare Gambles with National Security," in Cyberwar, 229.

[43] Kevin Soo Hoo, Seymour Goodman and Lawrence Greenberg, "Information Technology and the Terrorist Threat," Survival vol. 39, no. 3 (Autumn 1997): 149.

[44] James Kerr, "Information Assurance: Implications to National Security and Emergency Preparedness," in Cyberwar, 257.

"new" types of crime. The Justice Department has proposed that federal computer crime laws be changed to upgrade certain types of computer intrusions from misdemeanors to felonies and to expand the definition of criminal "damage" to include any impairment of data integrity or availability that might endanger public health and safety.[45] It is probable that as knowledge on potential IW damage increases, judicial laws will expand accordingly. Recently, a California federal court convicted a man for sending hate e-mails. Richard Machado was the first person to be prosecuted for what the government called an Internet hate crime.[46] In 1996, Machado had sent death threats to 59 Asian students at the University of California Irvine, blaming the students for campus crimes and demanding that they leave school, or be killed. He was convicted under a federal law against intimidating people from attending public places, in this case, free and unfettered use of the Internet.[47] In the face of increasing national dependence on information systems, federal laws protecting civilian access to those systems must increase dramatically in the future.

Other means of preserving our informational integrity involve developing infrastructure redundancy or contingency networks that would be utilized when the primary systems are degraded or destroyed. This information assurance alternative is practiced to some extent within the military, but as yet, is deemed neither cost effective nor necessary throughout all the private sector. Though vital for continuous military operations and effectiveness, commercial services, as currently developed, are not designed for "graceful degradation" of services or maintaining duplicate systems in the event of a primary system failure. The cost-benefit analysis approach of the commercial world has in the past deemed that the expense of maintaining multiple systems far exceeded the potential risk of a catastrophic, systemic failure. That analysis may be obsolete in the future, if warnings of the predicted ease with which an adversary can disrupt our NII prove true.

---

[45] Ibid, 261.

[46] Knight-Ridder, "U.S. Court Sends Message About Internet Threat," Washington Post, 12 February 1998, Sec. A4.

[47] Ibid, Sec. A4.

The Defense Science Board estimated that efforts to improve the survivability of the NII could range from $3 billion, for the development of a skeleton emergency information infrastructure, to roughly $250 billion to globally secure the entire infrastructure to DoD standards.[48] Rand's IW vulnerability study, discussed in Section III above, drew similar conclusions in recommending possible defensive measures. Participants in the Rand study showed *no support* for any extraordinary government actions such as shutting down the NII or seizing control of the media and Internet as a defensive measure to an IW attack.[49] They did, however, recommend the creation of a Minimum Essential Information Infrastructure (MEII), established to provide core, critical information systems support in the event of catastrophic failure to the NII regardless of whether the cause was a sophisticated IW attack or power failure due to adverse weather conditions. Development and sustainment of an MEII would be the coordinated responsibility of the actual members of the MEII. The study recommended a series of federally sponsored incentives to reward those network owners and operators who had established procedures for detecting IW attacks and reconstituting information services, thereby minimizing disruptive effects to critical functions.

Until society sees a clearly defined IW threat and understands the potentially disruptive ramifications it brings to daily computer-based business, the public may be unconvinced that increased government intervention or mandated security measures are even desirable, much less warranted. Rather than wait until a concerted IW attack against the U.S. rallies industry's support for increased attention to information infrastructure defense and protection, our government needs to provide the facts about our nation's vulnerabilities *today*. By providing critical information on our info-dependencies and risks, policy makers can muster both the support of, and assistance from, national subject matter experts in developing a credible, possibly impenetrable, IW defense.

---

[48] John Carlin, "A Farewell to Arms," Wired, May 1997, 220.

[49] Molander, Riddile, and Wilson, 32.

There have been some recent indications of progress. Defining the national security threat posed by IW and identifying solutions to protect America's critical information infrastructure from an IW attack were fundamental tasks issued by President Clinton in Executive Order 13010, which established the President's Commission on Critical Infrastructure Protection (PCCIP).

> Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.... Because many of these critical infrastructures are owned and operated by the private sector, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation.[50]

Recognizing the requirement for multiple agency participation in developing an comprehensive strategy, the commission consisted of representatives from the Departments of Treasury, Justice, Defense, Commerce, Transportation and Energy, and from the Central Intelligence Agency, Federal Emergency Management Agency, Federal Bureau of Investigations, and National Security Agency. The commission was given 15 months to present a detailed report to the President which would:

> Assess the scope and nature of the threats to critical infrastructures
>
> Determine legal and policy issues raised by efforts to protect infrastructures
>
> Recommend a national policy and strategy for protecting critical infrastructures from physical and cyber attacks.[51]

In October 1997, the PCCIP delivered a classified, 269 page report to the White House, detailing vulnerabilities and providing recommendations for improving infrastructure protection.[52] The proposals included (1) establishing a new "information and warning" office to identify and assess threats to both public and private computer networks, (2) doubling fiscal year

---

[50] President Bill Clinton, Executive Order 13010, July 1996, URL: <http://www.pccip.gov/eo13010.html>, accessed 15 January 1998.

[51] Ibid.

[52] John Harris, "Panel Urges Federal Government to Step Up Efforts Against Computer Terrorism," Washington Post, 21 October 1997, Sec. A9.

(FY) 1999 funds for research and development of counter-IW equipment, and (3) regulating encryption technology to give law enforcement agencies the ability to decode encrypted communications while investigating suspected criminal activity.[53] While the commission found no evidence of an imminent IW attack, they did find widespread opportunity to exploit infrastructure weaknesses -- opportunities that were increasing daily. Lastly, the commission reemphasized the importance of a collaborative effort between public and private organizations in implementing protective measures and in maintaining appropriate levels of information security.

A final method of defending against a potential IW attack is by preventing the attack from ever being launched. The possibilities and potential success of a strategy of deterrence in relation to IW is still relatively unexplored and untested. The effectiveness of such an approach would be largely dependent upon the nature and motives of the attacker, our ability to localize the attack, and our ability to project a credible deterrent policy that is backed by a persuasive and damaging promise of retribution. Paralleling our nuclear deterrent policy of mutually assured destruction (MAD), an effective IW deterrence policy needs to convincingly articulate that an IW attack on America would elicit an immediate, decisive and formidable response that would prove disastrous for any potential attacker. The U.S. policy on what constitutes an IW attack on the U.S., and what consequences an attacker could expect in response to such an attack, must be clear, unambiguous, and perhaps most important, legally and morally enforceable. Having only recently identified our vulnerabilities to an information attack, U.S. decision makers have been slow to devise and promulgate a policy of IW deterrence, possibly because they are reluctant to publicize our national vulnerabilities in this area. Additionally, at this stage it is difficult to characterize an IW attack as needing a dedicated deterrence policy until we are able to quantify its destructive potential to our national well-being. But it is imperative that U.S. policy makers identify, from a national perspective, what constitutes an "act of information war"

[53] Ibid.

against the United States. Until we do, we will limit our ability and our moral foundation to effectively respond to an overt IW attack.

V. RESPONDING TO AN IW ATTACK

The power and effectiveness of an informationally assisted military response was ably demonstrated during the Gulf War. The use of precision guided munitions and advanced command and control (C2) technologies seemed to dominate reports of the Allied coalition's victory during DESERT STORM. But even with a clearly defined adversary, whose repeated hostile actions rallied international support for an armed response, instances of non-combatant casualties and associated collateral damage evoked periods of unease and mission reevaluation among coalition partners. If wartime casualties can so greatly disturb the international community, even when an armed response is as justified and provoked as it was during DESERT STORM, how can the United States rally support for an armed response and its associated inevitable casualties? If an IW attack on the U.S. does not violate territorial waters, airspace or land, and results in no visible damage to buildings and no direct loss of life, does it meet the criteria of an invasion of U.S. sovereignty? Any U.S. response to an IW attack would need to be proportional and commensurate to the damage inflicted on our nation. An unduly harsh or bloody retaliatory response would be unacceptable to both the American populace and the international community. As one DoD official summarized, "What are we going to do, nuke them for turning off our TVs?"[54]

Information Warfare is a relatively new field without clearly established criteria for defining actions as acts of war, crime, or merely unethical behavior. Issues that need to be addressed when devising a national response to an IW attack include:

What level of NII disruption or destruction would constitute classification as an "Act of War" on the United States?

[54] Bruce Berkowitz, "Warfare in the Information Age," in In Athena's Camp: Preparing for Conflict in the Information Age, eds. John Arquilla and David Ronfeldt (Santa Monica, CA: The Rand Corp., 1997), 184.

How effective would a "retaliation in kind" be to an adversary with only minimal national dependence on information infrastructures?

Is it morally acceptable for the U.S. to respond with bombs and bullets to an attack that did not directly take American or Allied lives?

With what assurity can the United States identify the perpetrator of an IW attack to ensure that our measured response is directed at the "appropriate" adversary?

Can the U.S. form "information alliances" with other nations when our closest allies are also economic competitors, some of whom may condone or conduct certain forms of informational intrusion on other countries?

U.S. policy makers will need to quantify the nature and severity of an IW attack to distinguish between criminal acts of disruption best dealt with by law enforcement agencies and destructive informational acts of war that are designed to cripple a nation. The distinction will not be easy and could surely complicate the possibility of formulating a rapid response in the early phases of a perceived attack. To effectively identify a proportional and measured response to an attack, the *value* of the information lost, compromised or destroyed must be quantified. If telephone services are made inoperable for a week, would that constitute an act of war, or an act of "inconvenience"? Would deactivation of the 911 service, which would inevitably result in preventable civilian deaths, be a more sinister and heinous attack? What if manipulation of the air traffic control system resulted in multiple in-flight collisions of commercial airliners?

Obviously, the acceptability of an armed response will need to be proportional to the damage, or more accurately, to the *perceived* damage of an attack on the U.S. The difficulty in measuring that damage, and convincing the American public that a destructive response is warranted, may be extremely challenging.

With only a handful of countries, including the U.S., categorized as Third Wave post-industrial societies, the effectiveness of responding to an IW attack with a retaliatory IW "strike" will be limited. While many countries and non-state organizations will be able to cheaply and easily acquire offensive IW capabilities, their own national infrastructure will not necessarily be dependent on information age technologies and information networking. The threat of a

"retaliation in kind" would be neither a credible deterrent nor an overwhelmingly threatening response to the majority of these First and Second Wave societies. RAND published a general scaling of worldwide telecommunications connectivity during 1995. Employing a scale of 0 to 16, where 16 signified high connectivity, they found that much of Africa had zero connectivity and most of the Middle East and Southeast Asia received no more than a 4 rating.[55] To low tech societies such as these, an IW retaliatory strike by the U.S. would be of little consequence. It is therefore imperative in developing an IW deterrent that the United States maintain the prerogative to respond to an IW intrusion with both counter-IW and conventional military weaponry, as applicable. Our national intentions and convictions in choosing an appropriate response must be formulated, documented, publicized and defended well in advance of our ever even *requiring* a retaliatory response, so that our IW policy can act as a deterrent to any such attacks in the future.

Formulating a proportional response requires several key pieces of information. The first, most obvious requirement is that of identifying who is responsible for an IW attack. In the past, simply locating where an attack originated would be sufficient for pinpointing an attacker. Today, when information can be manipulated, and networked systems can mask the source of an electronic signal or command, the issue of identification is more complex. The previous section discussed our national limitations in tracing the sources of computer intrusions. Until methods are developed to help identify the true origin of an IW attack, we will be resigned to interpreting "patterns" or assessing possible motives to aid in identifying an IW attacker. But such subjective interpretations of adversarial motivations and actions would be insufficient in justifying a conventional military reprisal.

Determining the value of information lost or assessing the actual damage incurred from an IW strike on the U.S. will also be a critical requirement for gauging possible responses.[56]

---

[55] Richard J. Harknett, "Information Warfare and Deterrence," Parameters vol. 26, no. 3 (Autumn 1996): 96.

[56] Devost, 25.

When does disruption to an information infrastructure transition from an inconvenience to a significant threat to national security and economic stability? Our economic well being has always been of paramount national interest; its importance is evident in both our domestic and foreign policies. An IW assault on U.S. financial markets, assets and accounts could be devastating, and its impact would be felt not only nation-wide, but internationally. And yet, the defense of domestic financial institutions has traditionally been the responsibility of law enforcement agencies and have never required a military response in the past. The vulnerability of our economic "power base" to an overt IW attack might require its redesignation as a national asset whose targeting would constitute an act of war and whose protection would merit military attention. In the information age, where targeting lucrative national assets will likely replace a force on force interaction, responding to such attacks might better be designated as a military mission rather than one solely for civil law enforcement.

Some have questioned the ethics of U.S. employment of offensive IW strategies, whether in times of war, crisis, or peace. While there is little disagreement that the U.S. is vulnerable to IW attacks to varying degrees, concerns over the U.S. being the *originator* of an IW attack stem from questions on the manageability of an IW "weapon". Because of the networked structure of many national systems, an IW attack aimed at purely military targets may have a much broader footprint, and result in unintended consequences that the American people may not be willing to condone or accept. If the military is unable to *control* the sphere of impact from an IW assault, can that method of warfare be touted as truly non-lethal or precise? Even in the aftermath of the Gulf War, Iraqi civilian casualties sky-rocketed as a result of the destruction of Iraqi electric power systems by precision guided munitions.[57] Incontestably a military target, the destruction of the powerplant had far reaching implications long after the fighting was over. Without electric power, the water and sewage systems collapsed, which led to civilian deaths due to disease and malnutrition. Even with precision guided conventional weapons, the ultimate

[57] Stephen S. Rosenfeld, "The Human Costs," Washington Post, 20 February 1998, Sec. A23.

collateral damage effect was unanticipated. It may be even less likely that the precise location and effect of an IW attack could be predicted and controlled. As Martin Hill asserts, "An irony of IW is that it is almost always possible to do something, somewhere, sometime, but it is only rarely possible to do a specific thing, at a specific location, at a specific time."[58]

The Tofflers suggest a reevaluation of what they term the "norms of war and peace" in the face of the new Third Wave information capabilities.[59] They describe how past international agreements imposed necessary restrictions on Second Wave warfighting, to include regulations on the use of weapons of mass destruction, treatment of prisoners of war, and categorization of medical support personnel as neutrals during warfare. They suggest that until new, internationally accepted treaties, customs and regulations are developed and implemented globally to deal with Third Wave warfare capabilities, the U.S. will be handicapped in its attempt to respond to and employ its own IW tactics. When IW attacks are predominantly categorized as non-lethal, it may be necessary to lower the threshold of what constitutes an act of war, and what can be employed as a measured, proportional, and yet punitive retaliatory strike. Society's, and consequently the military's, traditional rules of engagement may become antiquated and obsolete in the information age. Likewise, the norms that govern escalation to armed conflict and escalation control will be affected with the addition of Third Wave warfare capabilities.

At present, the law of war, or law of armed conflict (LOAC), is inadequate to circumscribe the implications and impact of information warfare. While conventional attacks against information systems can be addressed using traditional LOAC guidelines, the use of new information weapons (viruses, logic bombs, trojan horses, etc.) and their targets are less clearly regulated. As currently recognized, the LOAC specifies, above all, *armed conflict*, a notion that is meaningless when discussing electronic attacks against electronic systems. Similarly inadequate in the Info Age, LOAC is predicated on the engagement of forces and the entry of

---

[58] Martin Hill, "It is Time to Get On With Information Warfare," Defense Intelligence Journal vol. 5, no. 1 (Spring 1996): 36.

[59] Tofflers, 224.

one nation into another's sovereign territory.[60] While adequate in scope to cover the possibilities of transnational hostilities in our recent past, such vernacular is no longer sufficient for encompassing the range of hostile actions possible to Third Wave societies.

As technology advances, noticeable gaps and inadequacies are emerging in previously acceptable regulations on ethical conduct, proportionality in war, minimization of damage to non-combatants, and delineation of hostile intent and acts of armed aggression. The growing complexity of the information age has outpaced needed adjustments to the international norms, codes and laws of warfare. And because of the truly global nature of information networking, economic interdependence, and coalition operations, an international forum is required to reevaluate current legalities and regulations in regards to warfare to bring them in step with the demands of a changing informational environment.

[60] Richard W. Aldrich, "The International Legal Implications of Information Warfare," Airpower Journal vol. 10, no. 3 (Fall 1996): 102.

VI. PROTECTING A NEW VULNERABILITY

Leveraging information age technologies and informational connectivity creates vast opportunities for advances in military operations, economic growth, and commercial efficiencies, but it also creates potentially serious vulnerabilities to our national security interests. Advanced technologies and the ease with which less powerful states can acquire them, has had a significant equalizing effect on the power and influence of nations. Information has emerged as a strategic asset worthy of conquest and destruction.[61] Informationally sophisticated and therefore informationally dependent nations will be more susceptible to disruptive IW attacks on their infrastructures than will First and Second Wave societies. Given the increased reliance of the U.S. public and private sectors on globally linked computer networks, U.S. information infrastructures have developed into lucrative and high payoff strategic targets. But fear of our inherent vulnerabilities must not preclude continued exploration and adaptation of emerging technologies into every facet of daily routine. The United States will be better served by concentrating efforts on identifying our national security weaknesses in the Information Age and developing a strong IW defense against possible exploitation of our emerging vulnerabilities.

To preserve the integrity, availability and security of national information infrastructures, an accurate assessment of our current and future vulnerabilities must be formulated and continually updated. Establishment of an information "Red Cell" to conduct wargames that probe national information systems and identify inherent weaknesses in their security measures should be an immediate step. Involving both private and public sector participation in Red Cell efforts will be a fundamental requirement as the majority of the NII depends on commercially developed and marketed parts and systems. By exposing industry to present day and near term system vulnerabilities, the private sector will be more apt to weigh system weaknesses as

---

[61] Schwartau, 13.

significant liabilities to effective and efficient business practices and work to eliminate identified vulnerabilities in subsequent technological versions.

Additionally, government should allocate sufficient funds into research and development efforts for enhancing computer security and infrastructure protection, and for activating an Indications and Warning Center that can accurately assess when an IW attack is attempted, limit its effects, and trace the origin of the attack. Those systems deemed critical to national security should have redundant component parts and databases that make up a Minimum Essential Information Infrastructure (MEII) that is increasingly resilient and impervious to an IW attack and system disruption or destruction. To encourage full scale efforts to improve infrastructure protection, governmental incentives and tax incentives could be made available to those companies and infrastructure caretakers who sufficiently fortify their systems.

Finally, government needs to energize an international forum, such as the United Nations, to codify rules and regulations governing the conduct of IW. National leaders will need to develop an informational "yardstick" to measure the value and merit of the intangibles -- information, knowledge, and cyberspace security -- to social well-being, economic prosperity and national security. By recognizing our critical and growing reliance on information age technologies, we will be better able to predict the impact of and prepare an appropriate response to, an information warfare attack on the homeland.

Despite its vulnerabilities, the United States is in the optimal position to capitalize on the immense advantages of information technologies by using them to promote human rights and democracy abroad, and project American ideals and opportunities to countries previously repressed or isolated from the international community. While current conditions of sporadic infrastructure connectivity may limit this approach against Third Wave societies, experts agree that totalitarian regimes will be hard pressed in restricting expansion of information technologies in the future. As global economies become increasingly interdependent and reliant on information-on-demand, nations that remain disconnected from the GII will be at a distinct disadvantage.

> As more and more human activities -- including all manner of commercial, social and governmental activities, throughout the private and public sectors -- move into cyberspace to take advantage of the efficiencies provided by interconnection, organizations and individuals who fail or refuse to connect will increasingly fall behind the pace of economic and social activity.[62]

Instead of allowing shrinking territorial "buffer zones" and vanishing international boundaries to work against us, the U.S. can leverage these inevitable changes to its benefit. The direction of President Clinton's 1997 National Security Strategy focused on efforts to enhance American leadership abroad and facilitate development of a stable and prosperous global community. Information age technologies and international interdependence -- technically, economically, politically, and informationally -- will be fundamental in realizing those goals.

---

[62] Hundley and Anderson, 33.

BIBLIOGRAPHY

Adams, Charlotte. "DoD Information Takes Big Strides But Still Lags Behind Threats." *Military & Aerospace Electronics,* vol. 8, no. 1 (January 1997): 17-20.

Aldrich, Richard W. "The International Legal Implications of Information Warfare." *Airpower Journal*, vol. 10, no. 3 (Fall 1996): 99-110.

Allard, Kenneth. "Assessing Byte City." *Washington Quarterly*, (Spring 1996): 87-89.

Arquilla, John and David Ronfeldt. "Cyber War is Coming." *Comparative Strategy*, vol. 12, no. 2 (Spring 1993): 141-165.

Arquilla, John and David Ronfeldt, eds. *In Athena's Camp: Preparing for Conflict in the Information Age.* Santa Monica, CA: The Rand Corp., 1997. 175-189.

Ayers, Robert. "Defensive Information Warfare: A Maginot Line in Hyperspace." *OSS Notices,* vol 2, no.10 (30 Dec 94): 8-15.

Campen, Alan D. "Assessments Necessary in Coming to Terms with Information War." *Signal,* (June 1996): 47-49.

_____. "Information, Truth and War." In *The First Information War.* Ed. Alan D. Campen. Fairfax VA: AFCEA International Press, 1992. 87-92.

Campen, Alan D., Douglas H. Dearth, and R. Thomas Goodden, eds. *Cyberwar: Security, Strategy and Conflict in the Information Age.* Fairfax, VA: AFCEA International Press, 1996.

Carlin, John. "A Farewell to Arms." *Wired*, May 1997, 51-58.

Chairman, Joint Chiefs of Staff. *Joint Vision 2010.* Washington, D.C.: GPO, 1996.

Chandrasekaran, Rajiv, and Elizabeth Corcoran. "Two California Teens Suspected of Breaking Into Government Computers." *Washington Post*, 28 February 1998, Sec. A6.

Clapper, James R. and Eben H. Trevino. "Critical Security Dominates Information Warfare Moves." *Signal,* (March 1995): 71-72.

Clinton, Bill. *Executive Order 13010.* July 1996, URL: <http://www.pccip.gov/eo13010.html>. Accessed 15 January 1998.

Cooper, Pat. "Cyberwar Recasts National Security." *Army Times,* (June 26, 1995): 26.

Devost, Matthew G. *National Security in the Information Age.* MA Political Science Thesis. VT: University of Vermont, May 1995.

Graham, Bradley. "11 U.S. Military Computer Systems Breached by Hackers This Month." *Washington Post,* 28 February 1998, Sec. A1.

Harknett, Richard. "Information Warfare and Deterrence." *Parameters,* vol. 26, no. 3 (Autumn 1996): 93-107.

Harris, John. "Panel Urges Federal Government to Step Up Efforts Against Computer Terrorism." *Washington Post,* 21 October 1997, Sec. A9.

Hill, Martin R. "It is Time to Get On With Information Warfare." *Defense Intelligence Journal,* vol. 5, no. 1 (Spring 1996): 25-41.

Hundley, Richard O., and Robert H. Anderson. *Security in Cyberspace: An Emerging Challenge for Society.* P-7893. Santa Monica, CA: The Rand Corp., Dec. 1994.

Joint Chiefs of Staff. *Joint Pub 1-02, Department of Defense Dictionary of Military and Associated Terms.* Washington, D.C.: GPO, 1998.

Kiras, James. "Information Warfare and the Face of Conflict in the 21st Century." *Peacekeeping* & *International Relations,* vol. unknown (Jul/Aug 96): 8-11.

Knight-Ridder. "U.S. Court Sends Message About Internet Threat." *Washington Post,* 12 February 1998, Sec. A4.

Mahnken, Thomas G. "War in the Information Age." *Joint Forces Quarterly,* (Winter 95-96): 39-43.

Mann, Paul. "Cyber Threat Expands with Unchecked Speed". *Aviation Week and Space Technology,* 8 July 1996, 63-64.

Minihan, Kenneth A. "Intelligence and Information Systems Security: Partners in Defensive Information Warfare." *Defense Intelligence Journal,* vol. 5, no. 1 (Spring 1996): 13-23.

Molander, Roger C., Andrew Riddile, and Peter Wilson. *Strategic Information Warfare: A New Face of War.* Santa Monica, CA: The Rand Corp., 1996.

Nunn, Sam. "Thinking Anew About U.S. Security." *Air Force Times,* 28 October 28 1996, 37.

Rona, Thomas P. "Information Warfare: An Age-Old Concept with New Insights." *Defense Intelligence Journal,* vol. 5, no. 1 (Spring 1996): 53-67.

Rosenfeld, Stephen. "The Human Costs." *Washington Post,* 20 February 1998, Sec. A23.

Schwartau, Winn. *Information Warfare: Chaos on the Electronic Superhighway*. New York, N.Y.: Thunder's Mouth Press, 1994.

Schwartzstein, Stuart J. *The Information Revolution and National Security Dimensions and Directions.* Washington, D.C.: The Center for Strategic and International Studies, 1996.

Scott, William B. "Information Warfare Policies Called Critical to National Security." *Aviation Week & Space Technology,* (Oct. 28 1996): 60-64.

Solomon, Richard H. "Information Revolution and International Conflict Management." *Peaceworks: Keynote Addresses from the Virtual Diplomacy Conference*, September 1997, 4.

Soo Hoo, Kevin, Seymour Goodman, and Lawrence Greenberg. "Information Technology and the Terrorist Threat." *Survival* vol. 39, no. 3 (Autumn 1997): 135-155.

Stein, George. "Information Warfare." *Airpower Journal* (Spring 1995): 30-39.

Sullivan, Gordon and James Dubik. *War in the Information Age.* Carlisle Barracks, PA: Strategic Studies Institute, 1994.

Szafranski, Richard. "A Theory of Information Warfare: Preparing for 2020." *Airpower Journal*, (Spring 1995): 56-65.

Szafranski, Richard. "When Waves Collide: Future Conflict." *Joint Forces Quarterly*, (Spring 1995): 77-83.

Toffler, Alvin and Heidi. *War and Anti-War: Survival at the Dawn of the 21st Century.* Boston, MA: Little, Brown and Co, 1993.

Van Riper, Lt Gen Paul K. and Maj Gen Robert H. Scales, Jr. "Preparing for War in the 21st Century." *Parameters,* vol. 27, no. 3 (Autumn 1997): 2-8.

Waller, Douglas. "Onward Cyber Soldiers." *Time,* 21 August 1995, 39-44.

The White House. *A National Security Strategy for a New Century.* Washington, D.C.: GPO, 1997.

Wriston, Walter B. "Bits, Bytes and Diplomacy." *Peaceworks: Keynote Addresses from the Virtual Diplomacy Conference*, September 1997, 6-10.